

# Certified SOC Analyst (CSA) - EC-Council

## Cours officiel, préparation à la certification CSA

Cours Pratique de 3 jours - 21h

Réf : ECQ - Prix 2024 : nous consulter

Le Certified SOC Analyst est une formation reconnue mondialement par les professionnels de la sécurité. Cette formation va vous plonger dans les processus et les technologies du SOC (centre opérationnel de sécurité) pour vous enseigner à penser comme un analyste de sécurité afin de mieux maîtriser les concepts de supervision et de détection.

### OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaître les missions d'un centre opérationnel de sécurité (SOC)

Maîtriser les fondamentaux sur les menaces de sécurité informatique et acquérir des compétences avancées

Connaître les outils, les stratégies et les procédures employées par les attaquants pour déterminer les indicateurs IOC

Surveiller et analyser des fichiers logs pour relever des alertes

Etre capable d'exécuter des événements de sécurité pour collecter, surveiller et analyser les logs

Savoir administrer des solutions SIEM (Splunk, OSSIM ou ELK)

Appréhender l'architecture, les types de déploiement et les paramètres avancés des solutions SIEM

Savoir développer un modèle de menaces et établir des rapports

Mettre en œuvre une surveillance et une analyse des menaces au sein d'une organisation

Savoir identifier les menaces qui émergent et lancer une analyse de sécurité

Transmettre des rapports d'incidents pour bénéficier d'un support supplémentaire

Savoir rédiger des rapports sur la méthode d'analyse utilisée et transmettre les résultats

Connaître les bases du processus de réponse aux incidents

Comprendre l'intérêt de l'association d'une solution SOC et IRT pour mieux gérer les incidents

### MÉTHODES PÉDAGOGIQUES

Animation de la formation en français.  
Support de cours officiel en anglais.

### TRAVAUX PRATIQUES

Ce cours est composé à 40 % de théorie et 60 % de mise en pratique.

### CERTIFICATION

Cette formation prépare à la certification Certified SOC Analyst. Le passage de l'examen est inclus dans le prix de la formation. L'examen consiste en un QCM de 100 questions (en anglais) d'une durée de 3 heures. Cette formation officielle est donnée exclusivement, en intra, par Advancia Training, ATC- Accredited Training Center officiel d'EC-Council, et par un formateur officiel CEI (Certified EC-Council Instructor). ITTCERT By ORSYS n'est pas ATC d'EC-Council.

### PARTICIPANTS

Analystes SOC, analyste en cybersécurité ou en sécurité des systèmes télécoms, réseaux et Informatiques, professionnels chargés de la gestion des opérations de sécurité ou de réseau.

### PRÉREQUIS

Connaissances sur la cybersécurité.

### COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

### MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.

Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.

Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...

À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur. Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

### MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

### MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

### ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

# LES DATES

---

Nous contacter